

FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER, L. L. P.

1300 I STREET, N. W.

WASHINGTON, DC 20005-3315

202 • 408 • 4000

FACSIMILE 202 • 408 • 4400

WRITER'S DIRECT DIAL NUMBER:

(202) 408-4096

December 26, 2000

ATTORNEY DOCKET NO.: 06944.0032  
CUSTOMER NUMBER: 22,852

**Box Patent Application**  
**Assistant Commissioner for Patents**  
**Washington, D.C. 20231**

New U.S. Patent Application

Title: A METHOD FOR PREVENTING KEY SHARE ATTACKS

being a **Continuation** of PCT International Application No. PCT/CA99/00595,  
filed on June 28, 1999

Inventors and Addresses:

1) Alfred J. MENEZES  
Waterloo, Ontario, Canada

2) Simon BLAKE-WILSON  
Toronto, Ontario, Canada

Sir:

We enclose the following papers for filing in the United States Patent and Trademark Office under 35 U.S.C. 111(a) as a **Continuation** application of PCT International Application No. PCT/CA99/00595, filed on June 28, 1999, which claimed priority of Canadian Patent Application No. 2,241,705, filed on June 26, 1998.

1. Application - 10 pages, including 1 independent claim and 7 claims total.
2. Copy of Cover Page of WIPO Publication No. WO 00/01109.
3. Drawing - 1 sheet of drawing containing 1 figure.
4. The filing fee is calculated as follows:

PTO  
U.S.  
09/745488  
12/26/00

011•813•3431•6943

BRUSSELS

011•322•646•0353

ATLANTA  
404•653•6400  
PALO ALTO  
650•849•6600

12/26/00  
jc685 U.S. PTO

00745488-133600

|   |                  |   |       |              |                                |           |
|---|------------------|---|-------|--------------|--------------------------------|-----------|
| Basic Application Filing Fee            |                  |   |       |              | \$710                          | \$ 710.00 |
|   | Number of Claims |   | Basic | Extra Claims |                                |           |
| Total Claims                            | 7                | - | 20    | 0            | x \$18                         |           |
| Independent Claims                      | 1                | - | 3     | 0            | x \$80                         |           |
| [ ] Presentation of Multiple Dep. Claim |                  |   |       |              | +\$270                         |           |
|   |                  |   |       |              | Subtotal                       | \$ 710.00 |
|   |                  |   |       |              | Reduction by ½ if small entity | -         |
|   |                  |   |       |              | TOTAL APPLICATION FILING FEE   | \$ 710.00 |

5. A check for \$710.00 is enclosed for filing fee.

Applicants claim the right to priority based on Canadian Patent Application No. 2,241,705, filed on June 26, 1998

Please address all correspondence with respect to this application to:

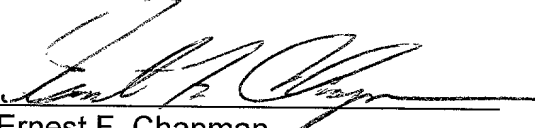
Finnegan, Henderson, Farabow,  
Garrett & Dunner, L.L.P.  
1300 I Street, N.W.  
Washington, D.C. 20005-3315

Please accord this application a serial number and filing date.

The Commissioner is hereby authorized to charge any additional filing fees due and any other fees due under 37 C.F.R. § 1.16 or § 1.17 during the pendency of this application to our Deposit Account No. 06-0916.

Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW,  
GARRETT & DUNNER, L.L.P.

By:   
Ernest F. Chapman  
Reg. No. 25,961

EFC/FPD/sci  
Enclosures